Towards the Automation of Data Networks

DOI: https://doi.org/10.15332/iteckne.v20i1.2918

ACCEPTED FOR PUBLICATION

The Editorial Board of ITECKNE journal approves the early publication of this manuscript since the editorial process has been satisfactorily completed. However, it warns readers that this PDF version is provisional and may be modified by proof-reading and document layout processes.

PUBLICACIÓN ANTICIPADA

El Comité Editorial de la revista ITECKNE aprueba la publicación anticipada del presente manuscrito dado que ha culminado el proceso editorial de forma satisfactoria. No obstante, advierte a los lectores que esta versión en PDF es provisional y puede ser modificada al realizar la corrección de estilo y la diagramación del documento.

Towards the Automation of Data Networks

Hacia la Automatización de las Redes de Datos

Santiago Cristóbal Pérez[1]; Higinio Alberto Facchini[2]; Bruno Alejandro Roberti-Ferri[3]; María Eugenia Stefanoni[4]; Matilde Inés Césari[5]

[1] Universidad Tecnológica Nacional, Mendoza, Argentina, santiagocp@frm.utn.edu.ar
[2] Universidad Tecnológica Nacional, Mendoza, Argentina, higiniofac@frm.utn.edu.ar
[3] Universidad Tecnológica Nacional, Mendoza, Argentina, broberti@frm.utn.edu.ar
[4] Universidad Tecnológica Nacional, Mendoza, Argentina, maria.stefanoni@frm.utn.edu.ar
[5] Universidad Tecnológica Nacional, Mendoza, Argentina, matilde.cesari@frm.utn.edu.ar

*Autor de correspondencia: Santiago Cristóbal Pérez; santiagocp@frm.utn.edu.ar

DOI del artículo: https://doi.org/10.15332/iteckne.v20i1.2918

ORCID Santiago Cristóbal Pérez: https://orcid.org/0000-0002-7241-3694
ORCID Higinio Alberto Facchini: https://orcid.org/0000-0002-3600-0438
ORCID Bruno Alejandro Roberti-Ferri: https://orcid.org/0000-0002-9986-2449
ORCI María Eugenia Stefanoni: https://orcid.org/0000-0003-0065-9297
ORCID Matilde Inés Césari: https://orcid.org/0000-0003-4786-7886

Fecha de recepción: 27 de mayo de 2022 **Fecha de aceptación**: 10 de septiembre de 2022

Abstract

A wide variety of enterprises, corporations, communications service providers (CSPs), and experts have highlighted the difficulty of managing modern networks. These networks exhibit high-impact technological innovations, such as cloud computing, mobility, new traffic profiles, network functions virtualization (NFV), the Internet of things (IoT), Big Data, among others. Network automation is a methodology in which physical and virtual network devices are automatically configured, provisioned, managed, and tested using software. Large enterprises such as Cisco, Juniper, Red Hat, and VMWare offer proprietary solutions for network automation. Additionally, the number of tools assisting in network automation has recently increased. Taken together, these developments have changed the way administrators build and manage networks. In this regard, most large communications operators are now working and moving toward truly autonomous networks that will eventually require an intensive use of Artificial Intelligence (AI). Advances in the area show that three specific segments —CSPs, Cloud Providers, and Enterprises— are all at different stages of automation maturity. Over time, network automation is expected to reach smaller organizations as well. This paper presents a specialized, detailed and current technical study on the state of the art in network automation, highlighting the trends observed in information technology (IT) environments, enterprises and communications operators —which are closely involved in this technology—, and concludes with a discussion on automation tools.

Keywords: artificial intelligence; automation platforms; automation tools; network automation

Resumen

Una amplia variedad de empresas, corporaciones, CSPs y especialistas han enfatizado la dificultad de gestionar redes modernas, que introducen innovaciones tecnológicas de alto impacto, como

cloud computing, movilidad, nuevos perfiles de tráfico, NFV, IoT, Big Data, entre otras. La automatización de redes es una metodología en la que los dispositivos de red físicos y virtuales se configuran, aprovisionan, administran y prueban automáticamente mediante software. Grandes empresas, como Cisco, Juniper, Red Hat o VMWare ofrecen soluciones propietarias de automatización de red. Además, recientemente ha habido un aumento en la cantidad de herramientas que asisten en la automatización de redes. Ambos hechos han marcado un cambio en la forma en que los administradores construyen y administran las redes. La mayoría de los grandes operadores de comunicaciones trabajan y tienden, en este sentido, a redes verdaderamente autónomas que, eventualmente, requerirán del uso intensivo de Inteligencia Artificial (IA). Los avances en la temática muestran que tres segmentos específicos CSPs, Proveedores en la Nube, y las empresas se encuentran en diferentes etapas de madurez de la automatización. Se espera, que progresivamente, esta tendencia alcance, también, a las organizaciones de menor envergadura. Este documento presenta un estudio técnico especializado, detallado y actual sobre el estado del arte en automatización de redes, destacando las tendencias que se observan en los entornos de TI, de las empresas y operadores de comunicaciones, más involucrados en esta tecnología y, finalizando, con una discusión sobre herramientas de automatización.

Palabras clave: automatización de red; herramientas de automatización; inteligencia artificial; plataformas de automatización

1. INTRODUCTION

Broadly speaking, automation is the action and effect of automating. In turn, the verb 'to automate' describes how a given set of actions can become automatic, i.e., how they can take place on their own without having someone directly participating in the process. In other words, automating a process means getting it to operate without human intervention by means of a feedback mechanism. Undoubtedly, these terms originated in the manufacturing industry, long before networks as known today even existed. However, while a given definition of network automation may still embody the general idea just described, many definitions of network automation differ in terms of scope and specificity entailed. In fact, a number of software vendors refer to them as automation tools, while others define them as configuration management tools, though both names seem to describe the same function. Network automation is described in [1] as "the process of automating the configuration, management and operations of a computer network. It is a broad term that includes a number of tools, technologies and methodologies used to automate network processes." A recent report by MIT Technology Review [2], drafted jointly with Ericsson [3], provides a more technical definition of this concept as "the elimination of repeatable manual tasks and their replacement by programmed tasks automated with the use of software." Examples of network automation include server configuration, maintenance scheduling, and the addition or elimination of services. Network automation that goes beyond a single server or service and involves the configuration of several virtualized network functions often entails carefully organizing workflow management across the network. A concrete example of this methodology is Vodafone's successful test [4] of full automation of its transport connectivity services.

In view of the above, in order to contribute to a better understanding of the definition and scope of Network Automation, this paper is structured as follows: Section 2 on Network Automation offers further details on the current context of the topic; Section 3 on Automation Networks Powered by AI describes the potential impact of AI on network automation; Section 4 on Automation Maturity in Communication Service Providers (CSPs), Cloud Providers, and Large Enterprises proposes differentiated levels of progress in network automation made by these organizations; Section 5 on Automation Platform Features provides a series of classifications and how to use such platforms; Section 6, Description of Some Automation Platforms, introduces some of the most widely known ones; and, finally, Section 7 summarizes the conclusions emerging from this study.

2 NETWORK AUTOMATION

2.1 Additional Concepts

In line with the concepts introduced earlier in this paper, the following additional terms will be used to accurately describe network automation:

- Closed loop: Blue Planet [5], a division of Ciena, defines closed-loop automation as "a continuous and repeating cycle of communications between the network infrastructure and software elements, including analytics, policy, and orchestration, to enable self-optimizing capabilities".
- Self-optimizing capabilities: self-optimization takes closed loops a step further, taking advantage of closed-loop processes to automatically adjust parameters and settings, resulting in an optimal use of limited resources such as information technology (IT) resources, radios, transport and access facilities, and energy.
- Autonomous network: although fully autonomous networks do not yet exist, members of TM Forum [6] define them as "providing the service lifecycle on demand with minimal or no human intervention".

With these concepts in mind, the goal of fully or almost fully autonomous networks comprises those networks that are configured, supervised, maintained, and repaired in an unattended manner, providing fully automated zero wait, zero touch, zero trouble network and information and communications technology (ICT) services for multiple vertical industries' sectors and consumers. A large portion of major CSPs and enterprises expect autonomous networks to eventually require Artificial Intelligence (AI) components to achieve this goal.

2.2 Benefits of Network Automation

One of the main hurdles for network administrators in organizations involves the increasing IT costs associated with network operations. The increasing amount of data, devices, and operations needed on said devices has started to exceed IT capabilities. In some cases, manual approaches prove insufficient or virtually impossible. As pointed out in [7], up to 95% of all network configuration changes are made manually, resulting in operational costs that may be 2 to 3 times the cost of the network assets per se. Each enterprise should assess their own situation in an attempt to keep up with the changes brought by the digital world, and decide whether it is time to increase automation and manage it remotely and in a centralized manner.

Network automation solutions may address a broad range of activities directly or indirectly, some of them being:

- Providing physical or virtual devices and services;
- Verifying devices and their configuration;
- Planning scenarios and managing IT inventory;
- Complying with configuration policies and guidelines of all network devices and services;
- Collecting network data related to devices, information systems, system programs, network topology, traffic, and services in real time;
- Analyzing data, including AI predictive analytics and Machine Learning (ML);
- Audited program updating, including software rollback if necessary;
- Repairing closed-loop network problems;
- Making information on incidents, panels, alerts, and alarms available;
- Enforcing security policies to a greater or lesser extent;
- Supervising the network and its services, ensuring the enforcement of service-level agreements (SLAs) between providers and clients.

It should be noted that automation has a few features of its own for these activities: 1) Automation tools can operate 24/7 with no interruptions, resulting in greater efficiency; 2) Automation helps collect large amounts of data, which, in turn, can be quickly analyzed to provide information that may

guide a given event or process; and 3) In a number of circumstances, an intelligent network automation tool can alter its behavior to attain some goal.

Enterprises that have pioneered the adoption of automation have derived multiple significant benefits:

- Lower costs: Because the underlying infrastructure is less complex, fewer man-hours are needed to configure, provision, and manage the network and its services.
- Lower probability of human errors: Potential errors associated with manual operation are reduced, such as configuration or typing errors, among others. Consequently, fewer staff members are required to solve these issues.
- Increased strategic workforce: By automating repetitive tasks, enterprises increase their productivity, improve their businesses and innovation, and create new employment opportunities for their current workforce.
- Reduced network downtime: Enterprises can attain higher levels of network availability, with the associated increase in productivity, improving their corporate image, and offering higher quality services.
- Accelerated development: It is possible to adopt new cloud-native applications and DevOps workflow processes through network management and security, which can be easily integrated into the development processes of these new applications.
- Accelerated implementation: The startup time of new applications and services can be reduced by automating provisioning and network management and security throughout the full lifecycle of applications, in data center and cloud environments.
- Deeper understanding about and control of the network: What takes place inside the network can be better understood and analyzed globally, promoting a more comprehensive assessment and the capacity for self-adaptation whenever necessary.

2.3 Research Lines

The academic sector also plays an active role by making significant contributions in software-defined networking (SDN), AI, ML, and simulation applied to network automation. This section presents a selection of studies showcasing the multiple scopes and perspectives to be found in network automation research. One of these studies [8] puts forth a common abstract model for an entire transport network, the standardization of design and deployment rules, and intent-based configuration. The aforementioned paper states this model should autonomously capture any status changes between the current and planned networks, and accept a variety of future network statuses and progressive implementations without affecting the current topology or network. However, another study [9] looks into the impact of the Internet of Things (IoT) and 5G technologies on current networks. These technologies are regarded to have led to the expansion of network scale and new applications. A Smart Integration Identifier Networking (SINET-I) is proposed, aimed at improving network automation capacity and promoting collaboration in heterogeneous networks.

An alternative approach, emerging from the programming languages used in network automation environments and platforms is presented in [10]. The study involved analyzing, in an experimental setting, the best method for improving the efficiency of the scripts applied to network devices. Additionally, a comparison was drawn between the time required for manual vs. automated configuration and the resulting differences in performance. The authors designed a network topology consisting of 36 Cisco devices with different Internetwork Operating System (IOS) versions, and concluded that the automated method reduces the time required by more than 90%. A different angle is presented in [11], in which SDN, in-band network telemetry (INT), and data analytics are combined to realize a closed-loop network automation system. The data plane and control plane design was experimentally demonstrated with a network system prototype consisting of six solar power distribution panels. The study concluded that closed-loop network automation can be achieved effectively.

Finally, 5G systems, automation, and intelligence in infrastructures are analyzed in [12], which also assesses the need for greater automation in the world of telecommunications. In that paper, the authors evaluated the scope of AI, Reinforcement Learning (RL), and Federated Learning (FL) in automated networks of the future.

2.4 Automation Levels

In their whitepaper, members of the Autonomous Networks Project [6] at TM Forum established six automation levels (Table 1) ranging from manual operations and maintenance to fully autonomous networks. The goal is to guide CSPs and large enterprises in assessing their current level of maturity, illustrating what their step-by-step progression might look like. Each level is based on the capabilities described for each category.

3 AI-POWERED NETWORK AUTOMATION PLATFORMS

In order to support the growing and increasingly complex, interconnected infrastructure, the IT industry is forced to change. In this sense, automation and analytics tools need to be combined, with AI being the key technology to merge them. Indeed, AI [13] constitutes the disruptive technology that is being used to support such convergence, exercising an impact on all areas of IT, including security, mobility, user experience, and management of the entire hardware and software infrastructure within IT.

AI, ML, Deep Learning (DL), Natural Language Processing (NLP), and Big Data, together with closed-loop automation, are used in the collection and automated normalization of data across all network domains and users, intelligent root cause analysis, and alerts for potential performance degradation or equipment malfunction. These technologies prove particularly useful for autocorrection in maximum availability, determining correlated events when deploying network virtual assistants, dynamically adjusting bandwidth, stopping or activating devices (whether functionally or electrically), predicting user experiences and understanding the anomalies that may affect their services (which often means problems can be solved before users are affected by them).

TABLE I
AUTOMATION LEVELS BY TM FORUM

LEVEL 5 - Fully Autonomous Network
The system has closed-loop automation capabilities, across multiple services, multiple domains (including partner domains), and the entire lifecycle.
LEVEL 4 - Highly Autonomous Network
In a more complicated, cross-domain environment, the system enables decision-making based on predictive analytics, or active closed-loop management, of service-oriented networks and customer experience.
LEVEL 3 - Autonomous Conditional Network
The system adapts to changes in the environment in real time and, in certain network domains, will optimize and adjust itself to the external environment, in order to enable closed-loop, intent-based management.
LEVEL 2 - Partially Autonomous Network

The system allows closed-loop operations and maintenance, for specific units based on AI modeling, under certain external conditions.
LEVEL 1 - Assisted Operations and Maintenance
The system executes a specific and repetitive substack, based on preconfiguration in order to increase execution efficiency.
LEVEL 0 - Manual Operations and Maintenance
The system releases assisted monitoring capabilities, but all dynamic tasks must be executed manually.

Source: The Authors

According to the annual report by TM Forum, in 2019, almost 50% of all CSPs around the world relied on AI to measure user experience. By 2021, this percentage had climbed to 85%. In line with this trend, CSPs in China were actively using AI by 2020, all the while shifting toward autonomous networks. For example, China Mobile [14] improved 5G resource utilization by automating massive multiple input, multiple output (MIMO) optimization. With AI, radio frequency (RF) utilization improved by 6%, while the aggregated traffic for the MIMO cell increased by 14.2%. Furthermore, the company has avoided around 2 million kg of CO2 emissions by switching mobile users to lower spectrum bands during times of little traffic and turning off high bands when they are not being used. China Telecom [15], on its part, managed to reduce energy consumption by 10%, relying on an intelligent system that would shut down cells, frequency bands and chipsets whenever they were not needed. This technology also uses AI-based anomaly detection algorithms to obtain early alerts for signaling storms in the central network, with a level of accuracy of 71% (signaling storms are similar to Denial-of-Service attacks on IP networks).

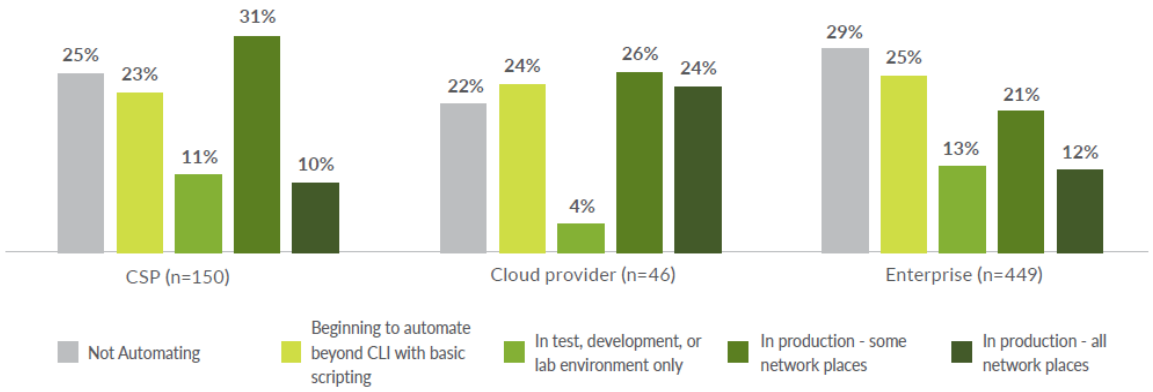
4 AUTOMATION MATURITY IN CSPS, CLOUD PROVIDERS, AND LARGE ENTERPRISES

The extent and manner in which specific organizations automate their networks differs depending on the dynamics of specific markets, the capacities available within the networks, the demands from users and clients, and the complexity of their infrastructure. Automation is to be achieved incrementally, although most organizations are now implementing it simultaneously across multiple business areas. A report by Juniper Networks [16] describes the differentiated penetration of network automation in CSPs, Cloud Providers, and Large Enterprises. According to the report, about 75% of CSPs, 71% of Large Enterprises, and 78% of Cloud Providers reported using some form of network automation (Fig. 1). Results show that these three segments are all at different stages of automation maturity, where about a quarter of each segment has begun to automate beyond the Command-Line Interface (CLI) with basic scripting. This, in turn, reveals that network automation is a lasting trend. Around 24% of Cloud Providers claim to use automation in production across all network places, even though nearly 40% are fairly new to this technology and have been using it for less than 3 years.

This situation is in sharp contrast with both CSPs and Enterprises, as only 10% of CSPs use automation in production in all network places (Fig. 2). This is to be expected, given the obvious limitations that come with the scale and complexity of large CSP networks. Meanwhile, Enterprises fall behind both types of service providers in terms of automation maturity, but resemble CSPs in terms of how long they have been using network automation. In 2019, improved security was the most common driver of this technology, but a couple of years later, all segments claimed that the top driver of automation was the reduction of hard and repetitive work (toil). Currently, business segments classify technology drivers very differently. Both types of service providers indicate that scaling network operational efficiency is the second most important technology driver, while improving metrics such as time to change and incident response, and mean-time-to-repair (MTTR) rank third and fourth, respectively.

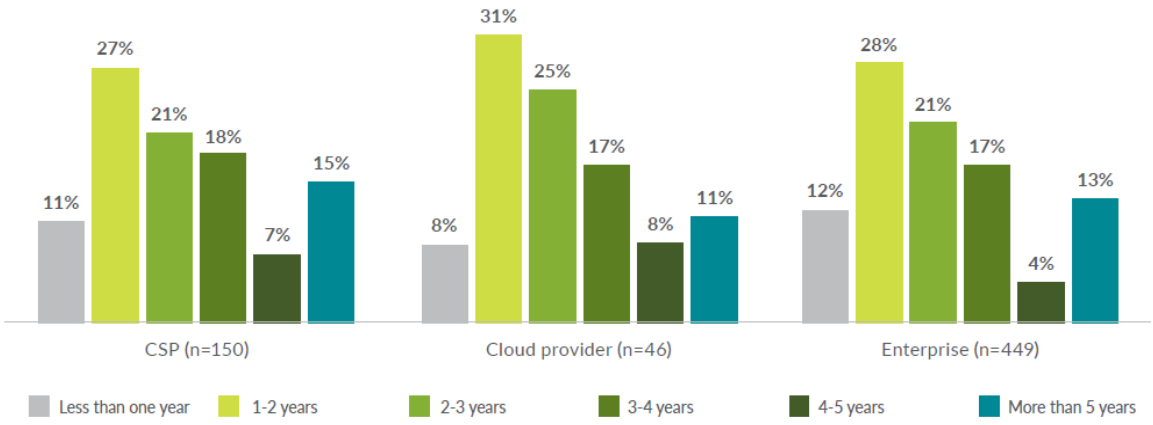
In light of the above, all three types of network enterprises automate network operations and establish their priorities very differently. The report by Juniper shows a thorough analysis of results related to network operations of Large Enterprises, CSPs, and Cloud Providers separately.
According to field experts, network automation is now turning into a necessity. Based on a recent survey by IDG [17] among IT leaders, automation is expanding rapidly in areas such as network provisioning and orchestration (56%), policy configuration (54%), and troubleshooting (50%).

Fig. 1. PERCENTAGE OF NETWORK AUTOMATION USE



Source: Adapted from [16]

Fig. 2. PERCENTAGE OF NETWORK AUTOMATION USE IN ALL NETWORK PLACES



Source: Adapted from [16]

5 AUTOMATION PLATFORM FEATURES

5.1 Access and Scopes

Automation platforms can be used across different types of networks, such as local area networks (LAN), wide area networks (WAN), cloud networks, data center networks, and wireless networks, in

any given context. Broadly speaking, each network automation tool can automate configuration changes in environments involving multiple providers.

For these environments, several interface categories, platforms, and protocols are used to execute script- or software-based network automation.

CLI has proven the traditional means to manually configure active equipment, as well as the basis or mechanism for network automation implementation. This interface is available for free, has been tested over time, and is highly customizable. A variety of open-source platforms offering network automation scripts are also available. These platforms typically have a library of commonly used workflows or CLI-like scripts, which can be easily replicated, ideally by using specific triggers and consistent procedures. In fact, platforms achieve this by running automated scripts to send changes to every device requiring them.

Rather than having a network administrator install Secure Socket Shell (SSH) in every router, switch, and firewall in order to manually modify text-based configurations, automation platforms can create configuration scripts (Fig. 3).

Because of their familiarity, legacy languages remain in network automation environments, for example, Perl and Tcl. However, as networks continue to become more complex, a number of open-source programming languages have gained popularity because of their extensive use and flexibility, such as Python and Ruby.

Fig. 3. EXAMPLE OF AUTOMATION SCRIPT

```
25  root.title('Python Remote Trackpad')
26  root.geometry('960x540')
27  global x, y, data
28  host = socket.gethostname()
29
30  server_socket = socket.socket()
31  server_socket.bind((host, port))
32  server_socket.listen(2)
33  conn, address = server_socket.accept()
34  print("Connection from: " + str(address))
35  x = 10
36  y = 10
37  def motion(event):
38      x, y = event.x, event.y
39      data = conn.recv(1024).decode()
40      data = str(x*2)+' '+str(y*2)
41      conn.send(data.encode())
42  root.bind('<Motion>', motion)
43  print(10)
44  cde = ''
45  def a(o):
46      conn.send('click'.encode())
47  def r(o):
48      conn.send('rclick'.encode())
```

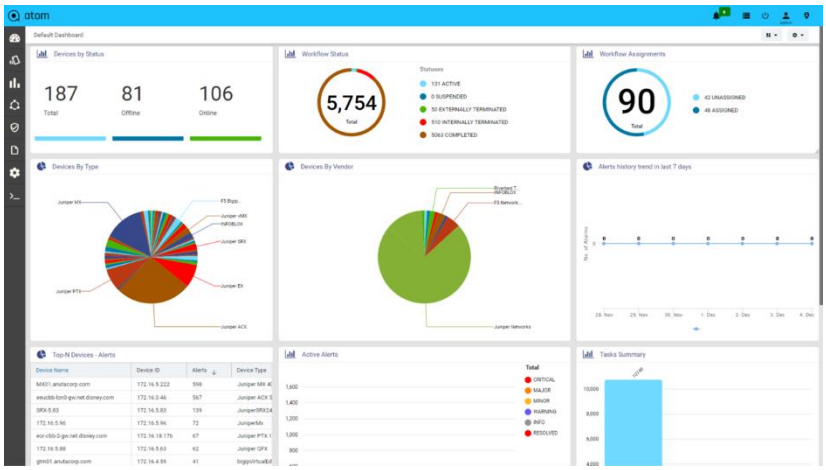
Source: The authors

Commercial network automation platforms are also available in the market. Most network equipment and infrastructure providers have their own software-based platforms, which offer significant automation capabilities by means of a dedicated application programming interface (API), mostly to

their own products, but also, to a lesser degree, to products by other manufacturers. This software-based network automation mode, sometimes referred to as intelligent network automation, is managed via an administration portal (Fig. 4) which eliminates the need to run scripts manually. In this case, platforms will generally provide forms or templates to create and execute tasks using simple language policies.

Based on the above, network automation platforms can adopt different styles and perspectives toward automation. However, they all share the primary goal of reducing the time spent on configuring simple and repetitive processes. Additionally, all platforms tend to support additional functions, which range from basic network mapping and network discovery, to more complex workflows, such as the administration of network configuration and the provisioning of virtual network resources.

Fig. 4. EXAMPLE OF A NETWORK ADMINISTRATION PLATFORM



5.2 Automation Platform Classification

A simple classification of automation tools, taking into account their origin, divides them into the following categories: (1) Infrastructure automation platforms, (2) Automation platforms with a specific purpose, and (3) SDN automation platforms. In practice, some platforms may fall under more than one of these categories.

5.2.1 Infrastructure Automation Platforms

This category covers platforms originally designed for application and server automation, which later evolved toward network automation. Many enterprises have used these tools for infrastructure and DevOps purposes, and IT staff is usually quite knowledgeable about them. Therefore, adding an automation component to an existing tool does not imply a significant effort in terms of implementation costs and the costs associated with the learning curve. Some of these automation platforms are more general upon comparing their network features and compatibility to different network hardware and software that are common in LAN configuration. However, they have been fully integrated to the other application and server automations used by organizations, and serve many purposes, such as performance monitoring, traffic and bandwidth analysis, configuration and change management, end-user monitoring and tracking, WAN performance monitoring, and IP address management. In other words, they provide a multi-purpose comprehensive solution in a single platform, even though they are not focused on networks per se.

5.2.2 Automation Platforms with a Specific Purpose

These are automation platforms designed specifically for network operations, which is why network administrators will find in them the most advanced features and functionality for network automation. Certainly, organizations using these platforms face the issue of having yet another tool used for a specific purpose only. These platforms, then, serve a much more limited purpose, such as managing the automated configuration of network devices. In this sense, they remain very useful and, as such, are often needed to comply with several regulatory standards. Additionally, several tools are available which offer different levels of automation across a variety of aspects. Broadly speaking, the more functions provided, the higher their price will be. In this case, it is worth evaluating whether any functions offered by different specific tools overlap with one another. For example, if a monitoring tool is in place, then an automation tool with a monitoring function is not likely to be necessary.

5.2.3 Software-Defined Networking (SDN) Automation Platforms

This last category refers to SDN which, together with network functions virtualization (NFV) technology, is used for network automation to configure and change the network according to business or service objectives.

Fortinet, Cisco, VMWare Velocloud, Citrix, Versa Networks, and CloudGenix are the most representative companies in terms of network solutions, which rely on SDN technology for traffic automation and optimization.
SDN manages the way in which hardware devices operate, allowing administrators to create virtual software networks between virtual machines and to manage multiple physical networks with networking software.

Automation platforms using SDN are designed to offer network and policy automation as well as network provisioning, monitoring, and segmentation from a single dashboard.
Through SDN, network automation can attain network administration objectives in the most effective manner.

6 DESCRIPTIONS OF SOME AUTOMATION PLATFORMS

A significant number of platforms are currently in use for network automation. As reported by specialized sites, some of them include: Red Hat Ansible Tower, Chef Enterprise Automation Stack, Puppet Enterprise, SaltStack Enterprise, BeyondEdge Networks, BMC TrueSight Automation for Networks, ManageEngine Network Configuration Manager, SolarWinds Network Configuration Manager, Juniper Apstra System, AppViewX ADC+, Itential Network Automation Platform, VMware NSX Intelligence, Cisco DNA Center, and HP Network Automation (HPNA). The following subsection presents a selection of three case studies representing the classification provided in 5.2.

6.1 Ansible Tower by Red Hat

Ansible, an open-source platform, was created originally for Linux-based system automation. The platform was acquired by Red Hat in 2015.

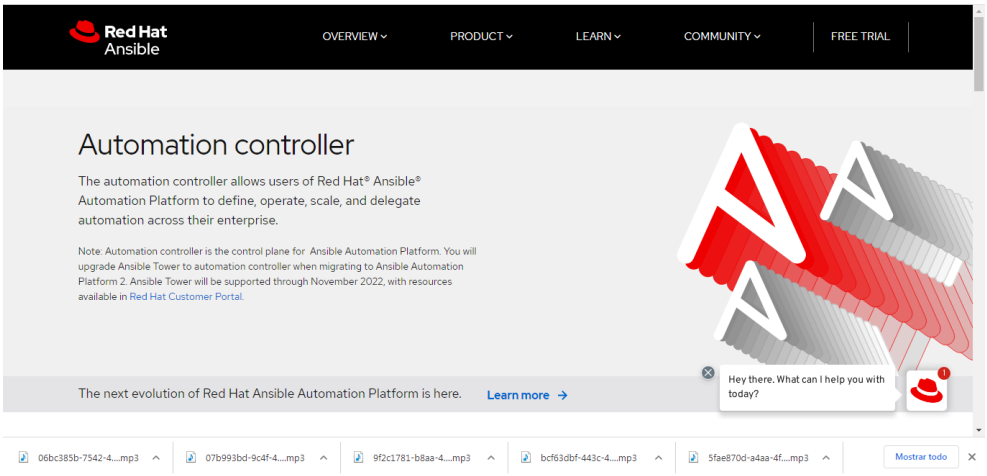
Since then, Red Hat has been including tool extensions with new features to automate other business IT infrastructure components, including network devices. In other words, the platform Red Hat Ansible Automation (Fig. 5) has served as the basis to achieve network automation within an organization.
When it comes to automation, Ansible Red Hat uses templates known as playbooks. In the open-source version, playbooks include CLI-like scripts, in order to create automation workflows. In the licensed version, known as Ansible Tower [18], a graphical user interface (GUI) is provided to

implement playbooks.

Ansible relies on an agentless architecture to communicate with network devices, via SSH or APIs, which makes it very suitable for proprietary systems.

Pre-built network modules are available that include automation templates for multiple providers.

Fig. 5. RED HAT ANSIBLE WEBSITE

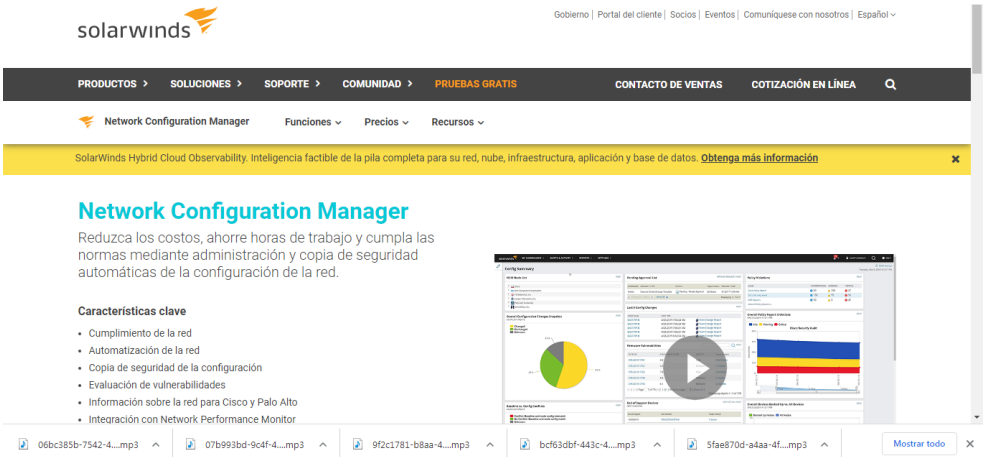


Source: The authors

6.2 SolarWinds Network Configuration Manager

This platform has been on the network automation market for many years now. Its product, SolarWinds Network Configuration Manager [19], is a compatible, heterogeneous, multi-vendor solution, especially for Cisco, Palo Alto, Juniper, HPE / Aruba, Dell, and F5 (Fig. 6).

Fig. 6. SOLARWINDS NETWORK CONFIGURATION MANAGER WEBSITE



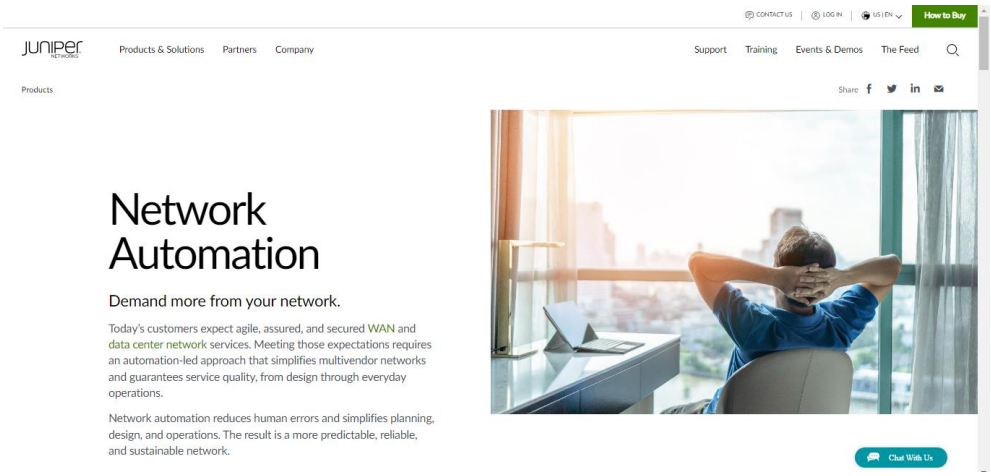
Source: The authors

The tool supports a significant number of network security capabilities, automatic backup and monitoring of configuration changes, and change approval and configuration auditing. Additionally, it can provide data on address configuration and administration, network fault level, bandwidth, performance, and network availability, all in one console. A unique functionality of this platform is its link to the US National Vulnerability Database, which allows it to automate the identification of non secure firmware. This feature can be used to enable services on network devices. Furthermore, SolarWinds Network Configuration Manager can be integrated with the vendor's wide range of products, such as the network performance monitor (NPM) tool. NPM constitutes a powerful software tool to diagnose, detect, and promptly solve network performance and downtime issues.

6.3 Juniper Paragon Automation

Juniper® Paragon Automation [20] (Fig. 7) is a module-based platform of cloud-native software applications that uses a web-based GUI, although it can also be installed as a local application. The following components may be integrated into the GUI: Paragon Pathfinder, Paragon Planner, Paragon Insights and Element Management Systems (EMS), as well as products by other vendors, all in a single control panel.

Fig 7. PARAGON AUTOMATION WEBSITE



Source: The authors

The platform provides network control functionalities through its integration with the Paragon Pathfinder module. This way, Paragon Automation functions as an SDN controller, allowing network administrators to manage an entire network in a centralized manner by running highly automated and programmable diagnostics on the device and by having analytics.

Additionally, administrators are given tools for offline visualization and a detailed architecture planning of their production network. Specifically, Paragon Planner serves to forecast the impact of network changes such as latency, additional traffic, and changes in traffic flows.

The Paragon Automation platform, which operates within a microservices architecture, uses Representational State Transfer (REST) APIs, Remote Procedure Call (gRPC) APIs, and other forms of messaging communications. Paragon Automation relies on ML to detect any anomaly or atypical value and to draw accurate predictions about the future behavior of both devices and networks.

7 CONCLUSIONS

Network devices such as routers, switches, and firewalls have traditionally been configured by a network administrator via command-line interfaces. In this scenario, every time a change or new feature emerges, configuration commands need to be entered manually across all relevant devices. Frequently, this approach is both time-consuming —which comes at a significant cost for organizations— and error-prone. This becomes a major issue when dealing with larger networks or more complex configurations.

Network automation amounts to automating routine or repetitive tasks in a network. Automation is a relevant process when incorporating network functions into the DevOps team. Network automation comes with a series of resources, tools, and benefits, which have been explained throughout this paper from a variety of angles. Currently, large enterprises as well as cloud and telecommunications service providers have been making consistent progress in this direction. Moreover, automation will certainly be extended to all enterprises, regardless of their current automation levels. In this sense, to a greater or lesser extent, depending on their priorities, every company will benefit from the advantages offered by automation.

REFERENCES

[1] Techopedia: Educating IT Professionals To Make Smarter. URL: *https://www.techopedia.com/*
[2] MIT Technology Review. URL: *https://www.technologyreview.com/*
[3] Ericcson. URL: *https://www.ericsson.com/en*
[4] Bodafone. URL: *https://www.vmware.com/content/microsites/possible/stories-uk/vodafone.html*
[5] Blue Planet Technology. URL: *https://www.blueplanet.com/technology/*
[6] TM Forum. URL: *https://www.tmforum.org/collaboration/autonomous-networks-project*
[7] Cisco, What is Network Automation?. URL: *https://www.cisco.com/c/en/us/solutions/automation/network-automation.html*
[8] T. Grahek, and A. Leong, "Network Automation for Design, Build and Operation at Scale," in *2019 Optical Fiber Communications Conference and Exhibition (OFC)*, San Diego, CA, USA, 2019.
[9] D. Chen, D. Gao, W. Quan, Q. Wang, G. Liu, and H. Zhang, "Promoting Network Automation for Heterogeneous Networks Collaboration," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, Victoria, BC, Canada, 2020.
[10] A. Mahmood Mazin, R. Ab Rahman, M. Kassim, and A. Razak Mahmud, "Performance Analysis on Network Automation Interaction with Network Devices Using Python," in *2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2021.
[11] S. Tang, H. Liang, M. Wang, T. Li, and Z. Zhu, "Closed-loop Network Automation with Generic Programmable Data Plane (G-PDP)," in *2021 International Conference on Computer Communications and Networks (ICCCN)*, Athens, Greece, 2021.
[12] L. Militano, A. Zafeiropoulos, E. Fotopoulou, R. Bruschi, and C. Lombardo, "AI-powered Infrastructures for Intelligence and Automation in Beyond-5G Systems," in *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain, 2021.
[13] OpenAI. URL: *https://openai.com/*
[14] China Mobile. URL: *https://www.chinamobileltd.com/en/global/home.php*
[15] China Telecom Corporation Limited. URL: *https://www.chinatelecom-h.com/en/global/home.php*
[16] The 2020 State of Network Automation. URL: *https://www.juniper.net/content/dam/www/assets/ebooks/us/en/the-2020-state-of-network-automation-report.pdf*
[17] IDG Connect. URL: *https://www.idgconnect.com/article/3639541/network-automation-where-do-you-begin.html*
[18] Ansible Tower. URL: *https://www.ansible.com/products/controller*

[19] SolarWinds Network Configuration Manager. URL: *https://www.solarwinds.com/es/network-configuration-manager*
[20] Juniper Paragon Automation. URL: *https://www.juniper.net/us/en/products/network-automation.html*